

The background of the entire page is a photograph of an industrial facility, likely a refinery or chemical plant, at night. The scene is filled with tall distillation columns, complex piping, and scaffolding, all illuminated by various lights. A semi-transparent grid pattern is overlaid on the entire image. In the upper left, the 'CYBERX' logo is displayed in a large, white, sans-serif font, with the 'X' being a larger, yellow-outlined character.

CYBERX

BATTLE-TESTED INDUSTRIAL CYBERSECURITY

CYBERX RELEASE NOTES

VERSION 2.7

Copyright © 2019, CyberX LTD.

This document contains proprietary and confidential information. All data submitted to the Customer is provided in reliance upon its consent not to use or disclose any information contained herein except in the context of its business dealings with CyberX Incorporated. The recipient of this document agrees to inform present and future employees of the Customer who view or have access to its content of its confidential nature.

The recipient also agrees not to duplicate or distribute or permit others to duplicate or distribute any material contained herein without CyberX express written consent.

CyberX retains all title, ownership and intellectual property rights to the material and trademarks contained herein, including all supporting documentation, files, marketing material, and multimedia.

Document version:

2.7 (0)

Last revised:

September 2, 2019

Contents

- 1 About CyberX Version 2.7 2**
 - Getting More Information 2
- 2 Scalability..... 3**
 - Sensor Interface Status Alerts Available..... 3
 - Upgrade Infrastructure – Streamlined Upgrade to Any Version..... 3
- 3 Visibility 4**
 - Enhanced Asset *Type* Classification 4
 - Asset Property Enrichment Using SNMP 5
 - Enhanced MAC Address Resolution 5
 - Firmware Data Displayed with Asset Properties..... 6
- 4 Ease of Use..... 7**
 - Access to User Guides from Consoles..... 7
 - Mute Alert Events..... 7
 - Enhanced Map Forensics 7
 - Smart IP/MAC Map Search..... 8
 - Analyze Assets with Specific Alerts..... 8
- 5 Upgrade Notes..... 10**

1 About CyberX Version 2.7

Version 2.7 provides important new features and feature enhancements that improve:


- Scalability
- Visibility
- Ease of Use

Users can upgrade to this version or install it as a first-time release.

Getting More Information

This document provides an overview of features made available with version 2.7.

For more information about features described in this document, refer to the Central Manager and Platform User Guides:

- At the CyberX Help Center: help.cyberx-labs.com.
- From the Console. To access the User Guide from the Console, select  and then select **Download User Guide**

For support and troubleshooting information, contact support@cyberx-labs.com.

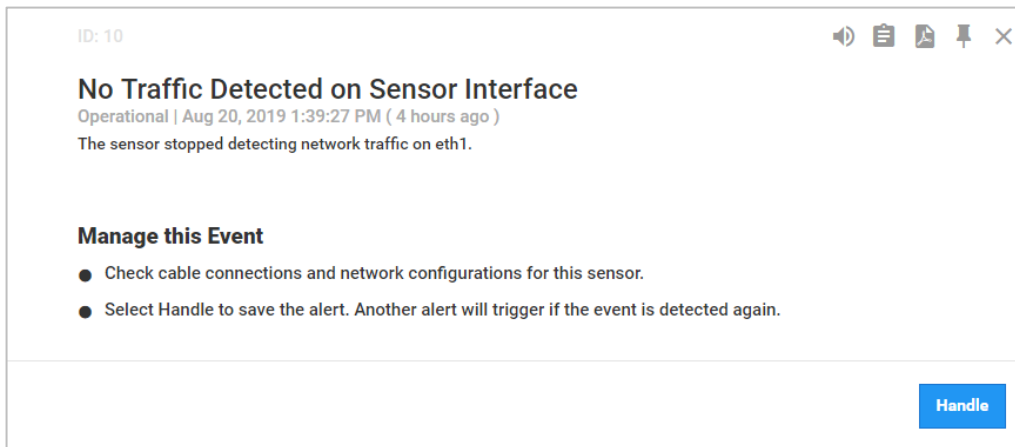
2 Scalability

The following scalability enhancements are available:

- [Sensor Interface Status Alerts Available](#)
- [Upgrade Infrastructure – Streamlined Upgrade to Any Version](#)

Sensor Interface Status Alerts Available

Users can now more easily monitor Sensor health with Sensor interface status alerts. Alerts are triggered if no traffic is detected on a Sensor interface, and when traffic resumes.



Component Support: CyberX Central Manager and Platform

Upgrade Infrastructure – Streamlined Upgrade to Any Version

The upgrade infrastructure has been improved and allows bridged, seamless upgrades over a series of versions. For example, upgrade seamlessly from version 2.7 to 2.10, without having to perform incremental upgrades. Bridged upgrades speed up the upgrade process. This infrastructure will be available when upgrading from version 2.7 to higher versions.

Component Support: CyberX Central Manager and Platform

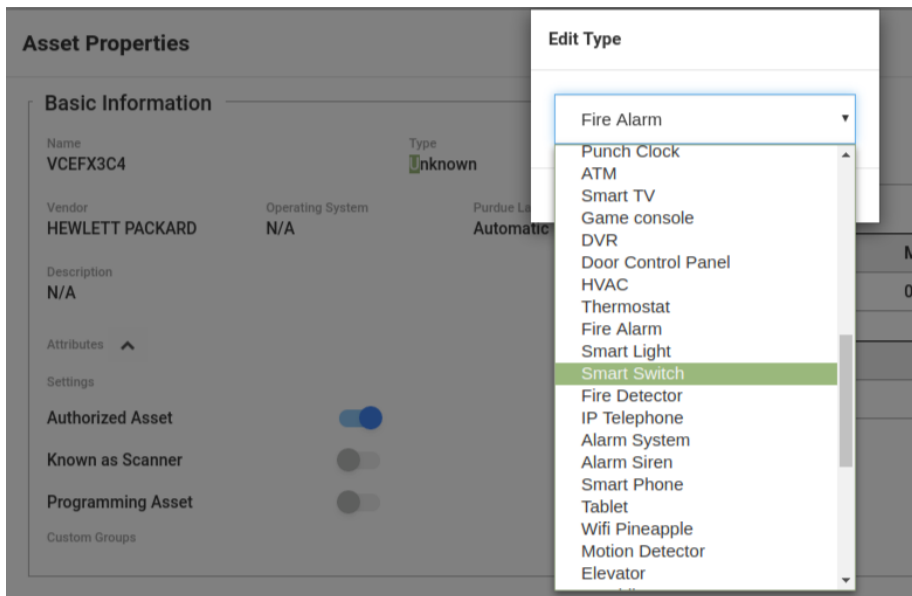
3 Visibility

The following visibility enhancements are available:

- Enhanced Asset Type Classification
- Asset Property Enrichment Using SNMP
- Enhanced MAC Address Resolution
- Firmware Data Displayed with Asset Properties

Enhanced Asset Type Classification

Enhance visibility by manually classifying detected assets with new device types.



The following new types can be assigned to assets.

■ ATM	■ Humidity Sensor	■ Protocol Converter	■ Smart TV
■ Backup Server	■ HVAC	■ Pneumatic Device	■ Uninterruptable Power Supply
■ Barcode scanner	■ Intercom	■ Punch Clock	■ Tablet
■ Control Panel	■ I/O Adaptor	■ Robot Controller	■ Turnstile
■ Door Panel	■ Marquee	■ Servo Drive	■ Variable Frequency Drive
■ DVR	■ Meter	■ Siren	■ Wifi Pineapple
■ Fire Alarm	■ Motion Detector	■ Smart Light	
■ Game Console	■ Phone	■ Smart Phone	
■ Fire Detector	■ People Counter System	■ Smart Switch	

Component Support: CyberX Platform

Asset Property Enrichment Using SNMP

CyberX now uses SNMP, as well as other monitoring methods, to resolve the following asset attributes:

- Name
- Type
- Vendor
- Operating System
- Firmware

SNMP discovery enriches the information available in the Asset in Inventory, Data Mining and other reports.

Enhanced MAC Address Resolution

Users can instruct CyberX to resolve MAC addresses when an estimated MAC/asset association is detected. This capability significantly improves MAC resolution for network assets and display of MAC information in the Console.

Previously MAC addresses were only resolved if a unique, definitive MAC address was detected for an asset.

Estimated MAC address resolution is carried out when the IP address of a new asset is associated with a specific MAC address for a configurable time.

To configure the MAC address resolution settings:

1. Select **Support > Engines** and then type **Educated MAC Guessing**.

The screenshot shows a configuration window titled "Edit Configuration". It contains a table with three rows of settings:

Name	Value
Educated Mac Guessing	0
Min Device Detection Time Minutes	10
Min Mac Detection Time Minutes	10

At the bottom right of the window, there are two buttons: "Cancel" and "Save".

This feature is not applicable for switches, HMIs or Engineering Stations.

Firmware Data Displayed with Asset Properties

Firmware details are available from the Asset Properties window. Previously this information was only available in the Asset Inventory.

The screenshot shows the 'Asset Properties' window for an asset with IP address 10.200.1.15. The window is divided into several sections:

- Basic Information:** Displays Name (10.200.1.15), Type (PLC), Vendor (N/A), Operating System (N/A), and Purdue Layer (Automatic). It also includes a 'Settings' section with three toggle switches: 'Authorized Asset' (checked), 'Known as Scanner' (unchecked), and 'Programming Asset' (unchecked).
- Network:** Shows the asset's state as 'SECURED'. It contains two tables:
 - Interfaces:** A table with columns 'IP Address', 'MAC Address', and 'Vendor'. The row shows IP Address: 10.200.1.15, MAC Address: N/A, and Vendor: N/A.
 - Protocols:** A table with a 'Name' column, showing 'BACNet'.
- Firmware:** A table with columns 'Address', 'Module Address', 'Model', and 'Firmware Version'. The row shows Address: 10.200.1.15, Module Address: Device Address: N/A, Net Address: N/A, Device ID: 1337, Model: BACnet Server, and Firmware Version: 00000.

If backplane information is resolved, the firmware details will not be displayed.

Component Support: CyberX Platform

4 Ease of Use

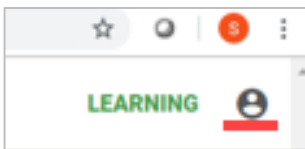
The following usability enhancements are available:

- [Access to User Guides from Consoles](#)
- [Mute Alert Events](#)
- [Enhanced Map Forensics](#)

Access to User Guides from Consoles

The User Guides for the Central Manager and Platform are now available directly from the product Consoles. Use the guides for quick access to product information.

To access the User Guide from the Console, select  and then select **Download User Guide**.



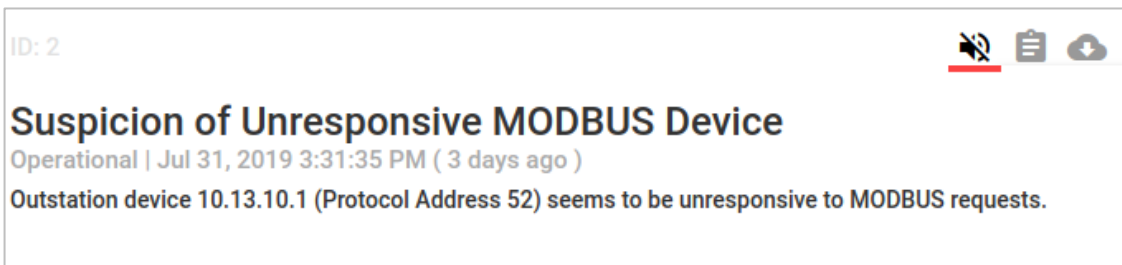
Mute Alert Events

Under certain circumstances, you may want to instruct your Sensor to ignore a specific scenario on your network. For example,

- The Anomaly engine triggers an alert on a spike in bandwidth between two assets, but the spike is valid for these assets.
- The Protocol Violation engine triggers an alert on a protocol deviation detected between two assets, but the deviation is valid between the assets.

In these situations, learning is not available. When learning cannot be carried out and you want to suppress the alert and remove the asset when calculating risks and attack vectors, you can mute the alert event instead.

Once muted, activity detected with identical assets and comparable traffic will not trigger additional alerts. Toggle the **Mute** icon from the alert message to suppress/activate the alert.



Component Support: CyberX Manager and CyberX Platform

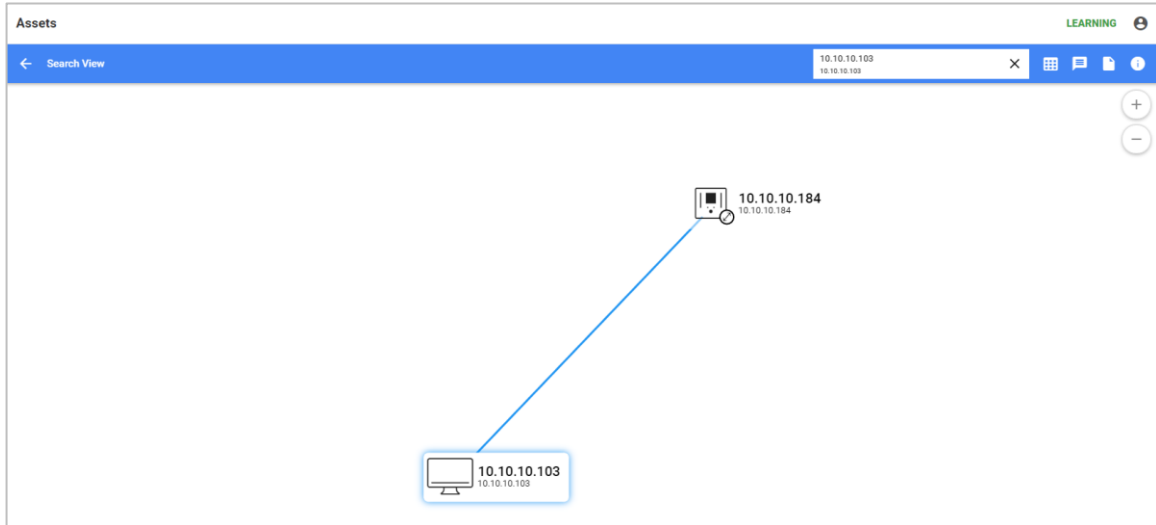
Enhanced Map Forensics

Map enhancements enable improved forensics on assets of interest:

- [Smart IP/MAC Map Search](#)
- [Analyze Assets with Specific Alerts](#)

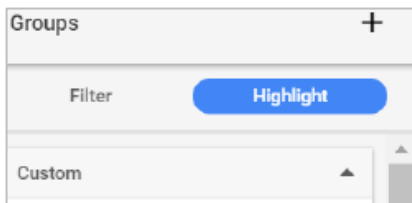
Smart IP/MAC Map Search

The IP/MAC map search provides smarter filtered results. Now when searching, the map drills directly to the IP or MAC queried and connected assets only. Previously the map displayed all assets in the subnet of the queried asset.



Assets are displayed in the new **Search View**. Select **Assets** to return to an unfiltered view of the queried asset.

This capability is available when the Map>**Highlight/Filter** options are disabled.



Analyze Assets with Specific Alerts

The new map *Alert View* lets you quickly gain insight into assets that triggered alert events.

When selecting an asset directly from an alert, the map automatically filters to the selected alert and assets connected to it.

The Quick Properties dialog box for the assets detected in the alert is displayed in the map as well.

ID: 5

RPC Operation Failed

Operational | Aug 20, 2019 6:43:05 PM (21 hours ago)

An RPC server error or an invalid RPC request was detected. RPC server 10.0.0.3 returned a Fault message to client 10.0.0.100.

Manage this Event

- Contact your IT and Security teams to verify that the RPC services are running properly. For example, that RPC is enabled and connected to the network. Also verify that the client has permission to access the server.
- Select Handle to save the alert. Another alert will trigger if the event is detected again.

Handle

Assets

Alert View Search by IP / MAC

XP-123
Type: Workstation
Vendor: VMWARE INC.
Operating System: Windows XP
Protocols: (Active Directory Services) (DNS) (LDAP) (RPC) (RPC Endpoint Mapper) (Windows Security Service)
IP Addresses: (10.0.0.10)
Mac Address: (08:00:2B:01:02:03)
Last Activity: 23 hours ago

abc
Type: Domain Controller
Vendor: VMWARE INC.
Protocols: (DNS) (RPC) (LDAP) (Active Directory Services) (Active Directory Services) (Active Directory Services) (RPC Endpoint Mapper) (Windows Security Service)
IP Addresses: (10.0.0.3)
Mac Address: (08:00:2B:01:02:03)
Last Activity: 23 hours ago

Component Support: CyberX Platform

5 Upgrade Notes

This version updates the VLAN configuration behavior.

Unused VLANs will no longer be displayed in the VLAN configuration screen, Map, Data Mining and other reports. Previously all VLANs were displayed.

Edit VLAN Configuration

VLAN Names	1	Infrastructure
	2	Unit 7 PL 12 ×
	27	Unit 5 PL 17 ×
	50	Unit 8
	117	Unit 9
	302	Unit 10
	1300	Unit 11
	1301	Manufacture
	1305	Name

[Add VLAN](#)

Close Save